Notice of Allowability	Application No.	Applicant(s)	
	09/728,800	MACHE, NIELS	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the Requet for Continued Examination (RCE) received on September 8, 2006*.

2. ☒ The allowed claim(s) is/are *5,8-10,15,18 and 19*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *12/08/2006* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

2. Authorization for this examiner's amendment was given in a telephone interview with Joseph Wrkich (Reg. No. 53,796) on December 8, 2006.

The application has been amended as follows:

3. Claims 1-4, 11-14, 20-24, and 26-27 are cancelled by virtue of this Examiner's Amendment.

Claim 5 (Currently Amended):

A method for the authenticated transmission of messages, comprising the following communication setup steps:

generating a login key by a keyed-hashing method on the basis of random data, temporal validity information, and a private key;

transmitting the login key from an originator to a destination; and

verifying the authenticity and the temporal validity of the login key on the basis of the keyed hashing digest on the destination side; and

comprising the following acknowledgement steps:

~~*in case the verification of the authenticity and the temporal validity of the login key is positive,*~~

generating an acknowledgement by a keyed-hashing method on the basis of second random data and the private key, wherein the acknowledgement key includes a time stamp;

transmitting the acknowledgement key from the destination to the originator; and

verifying the acknowledgement key by the originator, including checking the acknowledgement key on the basis of the time stamp and the previously stored temporal validity information whether the acknowledgement key is still valid,

wherein the keyed-hashing technique uses random data that is stored by the destination in a table during the temporal validity of the ~~data~~ login key.

Claim 15 (Currently Amended):

The distributed system for the authenticated transmission of messages, comprising:

an originator designed to generate a login key by a keyed-hashing method on the basis of random data, temporal validity information and a private key, wherein the login key includes a key hashing digest; and

a network for transmitting the login key from the originator to a destination, wherein the destination is designed to verify the authenticity and the temporal validity of the login key on the basis of the keyed hashing digest;

wherein the destination is designed to generate an acknowledgement key by a keyed-hashing method on the basis of second random data and the private key and to transmit the acknowledgement key to the originator ~~in case the verification of the authenticity and the temporal validity of the login key is positive,~~ and the acknowledgement key includes a time stamp;

the originator is designed to verify the acknowledgement key, including checking on the basis of the time stamp and the previously stored temporal validity information whether the acknowledgement key is still valid; and

the keyed hashing technique uses random data that is stored by the destination in a table during the temporal validity of the ~~data~~ login key.

REASONS FOR ALLOWANCE

4. Claims 5,8-10, 15, and 18-19 are allowed.

5. The following is an examiner's statement of reasons for allowance:

6. The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claims limitations in combination with the specific added limitations, as recited in independent claims 5 and 15 shown above, and subsequent dependent claims.

7. The Cited Prior Art (CPA), Misra et al. (U.S. Patent 5,757,920) in view of Haber et al. (U.S. Patent 5,781,629), does not teach nor suggest a method or system for verifying the authenticity and temporal validity of a login key at a destination sent by an originator, and generating an acknowledgement key by the destination by a keyed hashing technique on the basis of random data stored at a table at the destination, wherein the acknowledgement key includes a time stamp, and wherein the acknowledgement key is transmitted to the originator where it is verified on the basis of the time stamp and the previously stored temporal validity information.

8. The present invention provides the following advantages over prior art security systems and/or methods:

1) provides a method for reducing the risk of copy or replay attacks in the first step of a communication method in a more efficient way.

9. Thus this invention provides a way to reduce the likelihood of a replay attack in the first step of communication setup, by providing a login key which has a temporal validity associated with it at the originator, which is then sent to the destination. The destination then verifies the authenticity of the login key and checks the temporal validity before generating an acknowledgement key which has a time stamp and sending the acknowledgement key to the originator where it is verified and the temporal validity is checked to see if the key is still valid.

10. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

12/08/06
KA
12/07/2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100